ViPNet xFirewall 5 и 6 поколения — когда нужно реально импортозаместить NGFW

Алексей Данилов

Руководитель продуктового направления

инфотекс ТЕХНОДЕСТ

Синий поток

Новые возможности версии 5.6.4

инфотекс

Что нового в 5.6.4

1 Улучшенный механизм SSL/TLS-инспекции

2 Расширение возможностей агрегированных интерфейсов

3 Улучшенный пользовательский интерфейс

4 Поддержка новых аппаратных платформ

Что нового в 5.6.4

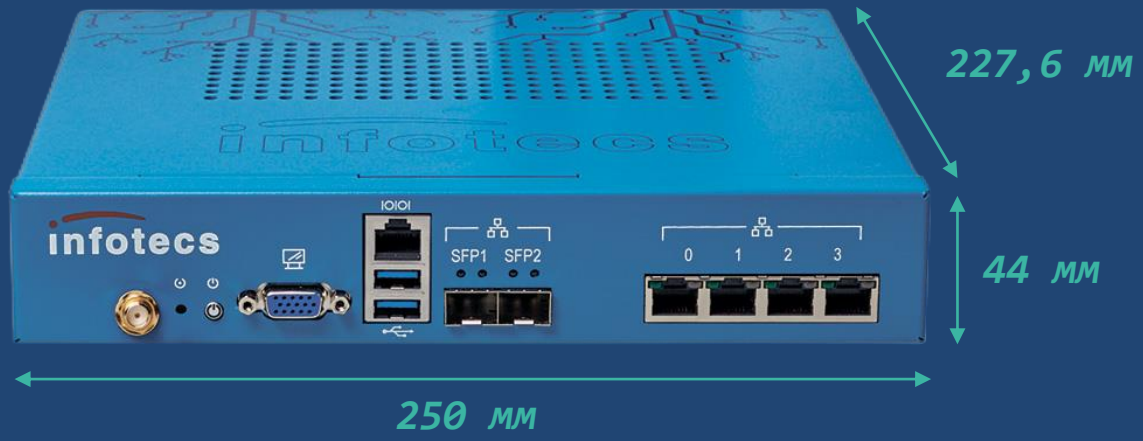
5 Сброс к заводским настройкам

6 RADIUS-аутентификация для SSH-подключений

7 Повышена скорость и стабильность отправки CEF-сообщений

8 Исправление ошибок

xF100 Q1/Q2



6 сетевых интерфейсов:

- 4 x 1 Гбит/сек RJ45
- 2 x 1 Гбит/сек SFP

Незначительно повысилась производительность

Производительность

Исполнение	xF100 N1	xF100 Q1/Q2
Firewall, 1518 Байт UDP (Мбит/сек)	722	**1 600**
Firewall, TCP Multistream (Мбит/сек)	600	**1 380**
AppControl (Firewall+DPI), (Мбит/сек)	180	**395**
NGFW (FW+DPI+IPS) (Мбит/сек)	13	**40**
NGFW+SSL Inspection (1МБ)	32	50
Firewall Throughput (UDP 64 Байт)	79 000	**137 000**
Connections per Second	10 000	**18 000**
Concurrent Connections	149 993	499 994

Производительность

Исполнение	xF1000 Q7/Q8	xF5000 Q2
Firewall, 1518 Байт UDP (Мбит/сек)	7 600	51 000
Firewall, TCP Multistream (Мбит/сек)	11 000	33 000
AppControl (Firewall+DPI), (Мбит/сек)	2 600	7 800
NGFW (FW+DPI+IPS) (Мбит/сек)	480	1 300
NGFW+SSL Inspection (1МБ)	480	1 300
Firewall Throughput (UDP 64 Байт)	2 200 000	4 000 000
Connections per Second	53 000	106 000
Concurrent Connections	4 999 000	29 999 990

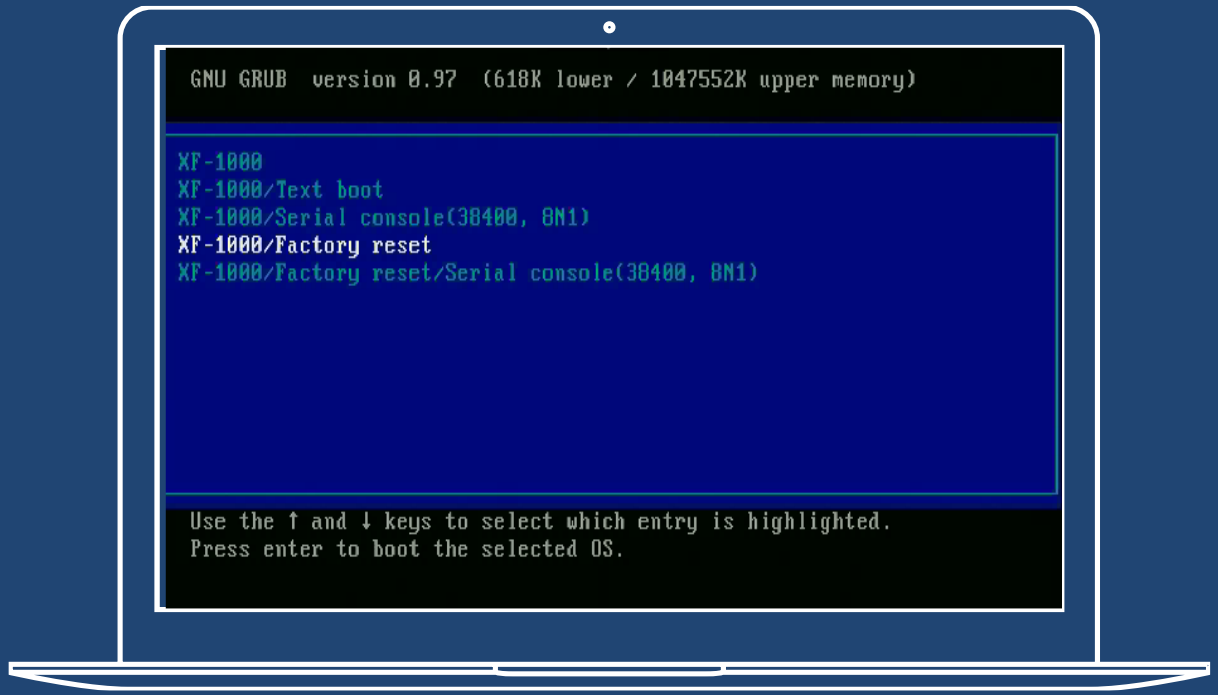
Radius-аутентификация

- Чтобы пользователь подключался к ViPNet xFirewall в режиме администратора, установите значение атрибута shell:priv-lvl равным 15.
- При другом значении атрибута shell:priv-lvl или при его отсутствии подключение будет выполняться в режиме пользователя.

Возможность возврата к предыдущей версии ViPNet xFirewall

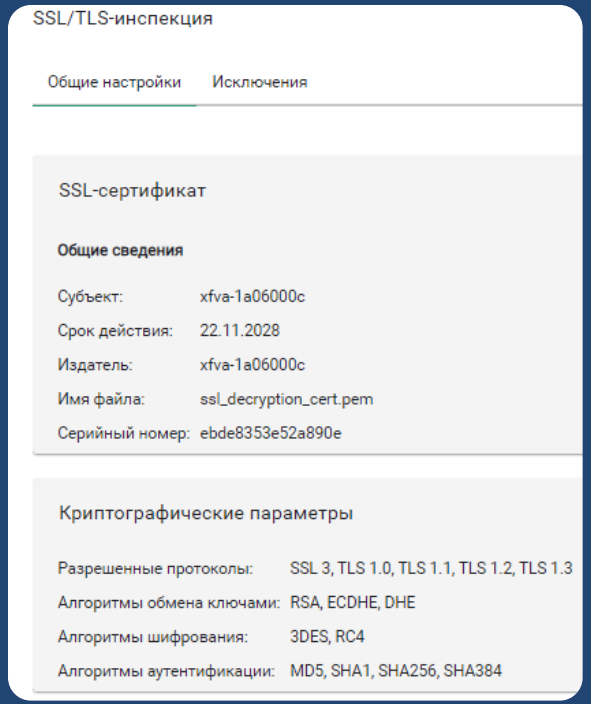
В ViPNet xFirewall добавлена возможность возврата ПО к версии 5.4.0

Сброс к заводским настройкам



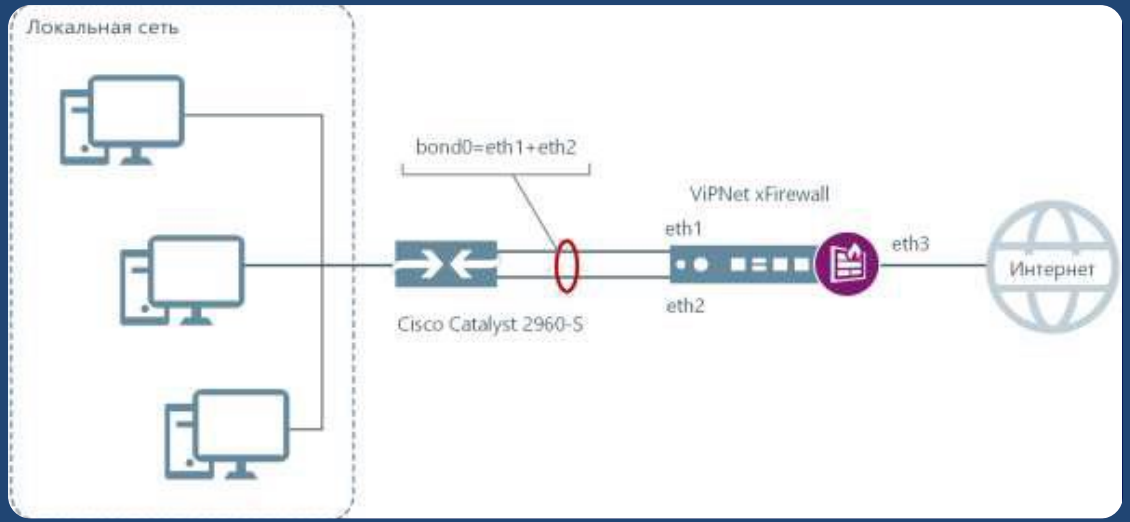
В строке «Are you sure you want to execute this command and delete key?» Введите «Delete», нажмите «Enter».

Улучшения SSL Inspection



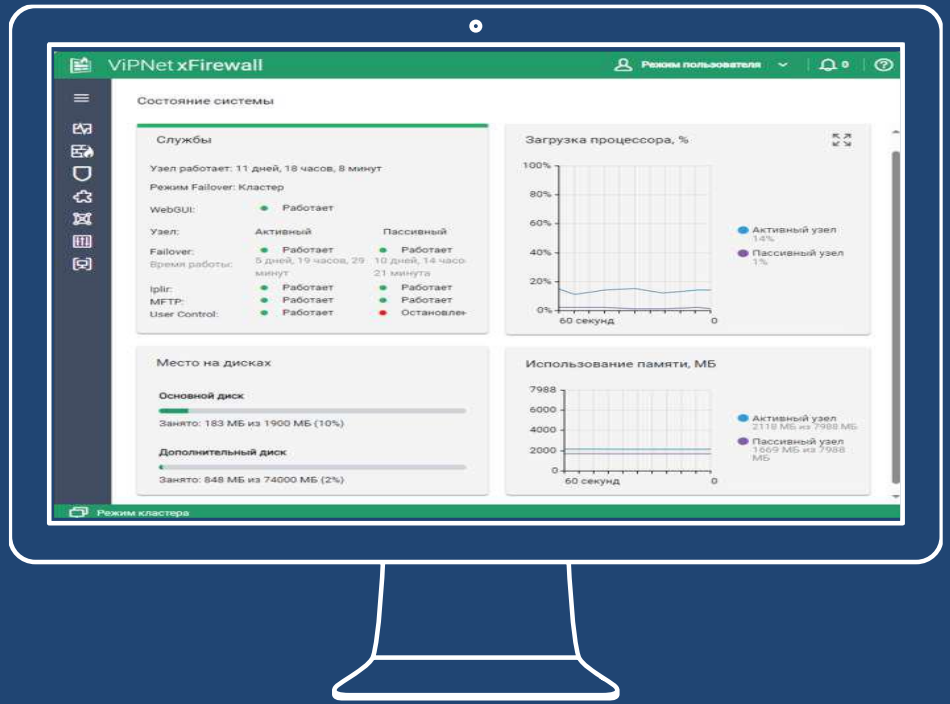
- Добавлена поддержка расшифровывания протокола TLS 1.3
- Добавлена возможность инспекции трафика HTTP/2
- Добавлены настройки доверия к сертификатам ресурсов:
  - проверка срока действия сертификатов;
  - проверка полей сертификата, определяющих его использование (key usage, extended key usage);
  - проверка самоподписанных сертификатов.
- Исключать из инспекции веб-ресурсы, используя их альтернативные имена (SAN – Subject Alternative Names) и поддомены (wildcard).

Агрегация интерфейсов



- Ранее вы могли включать в состав агрегированного интерфейса только до трех подчиненных физических. Теперь это ограничение снято.
- Максимальное количество агрегированных интерфейсов увеличено до 8.

Изменен вывод контролируемых параметров

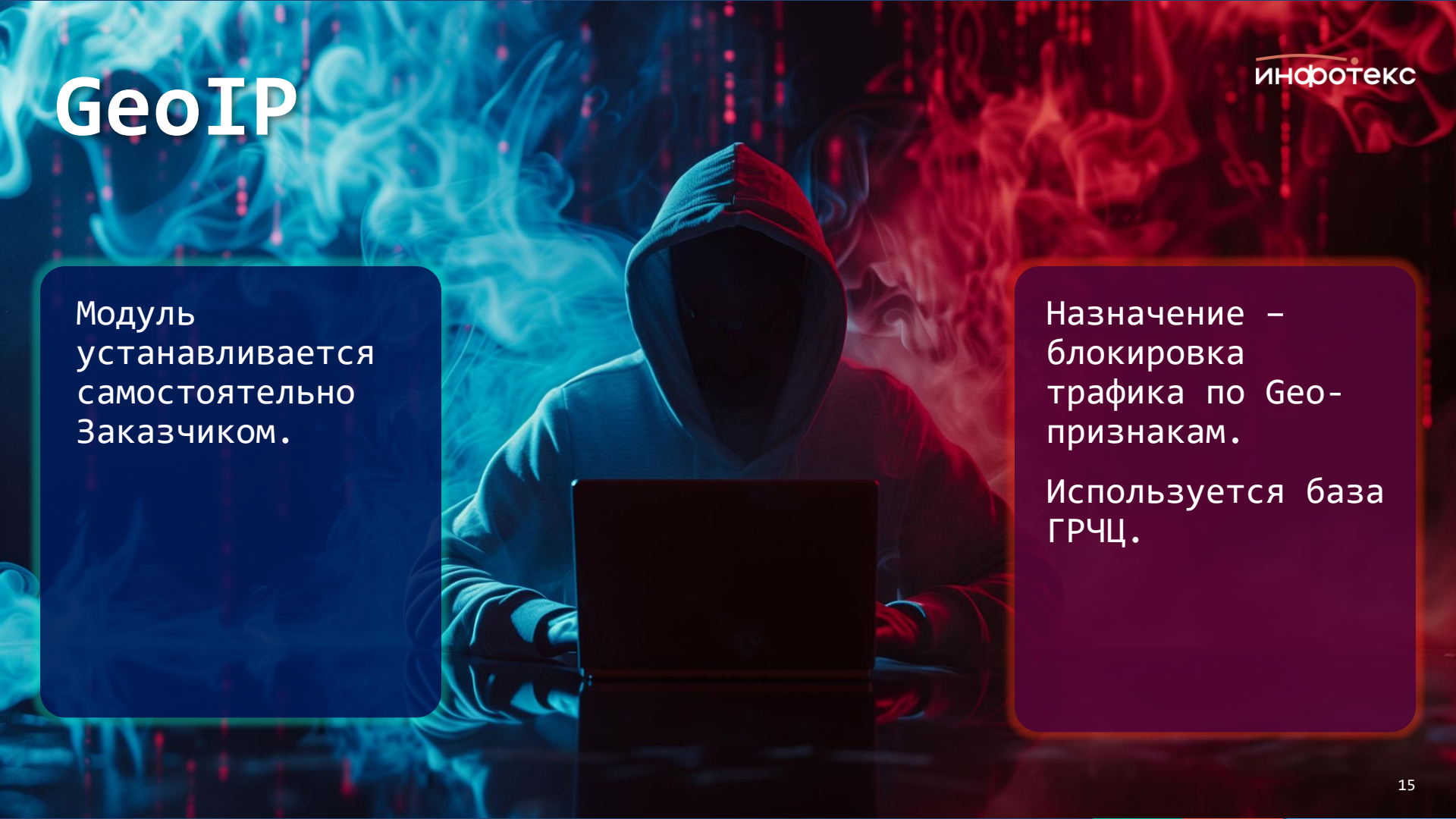


Теперь отображается относительная загрузка CPU, а максимальная загрузка всех ядер принята за 100%.

ViPNet xFirewall Add-ons

инфотекс

GeoIP



Модуль устанавливается самостоятельно Заказчиком.

Назначение – блокировка трафика по Geo-признакам.

Используется база ГРЧЦ.

Принципы GeoIP-фильтрации трафика

Модуль GeoIP-фильтрации

Модуль ViPNet xFirewall, позволяющий разграничивать доступ на основе геолокации. Блокирует входящий трафик из заданных регионов.

Первый этап анализа трафика

Это снижает долю трафика, анализируемого DPI, IPS, что повышает эффективность межсетевого экрана.

Белый список

Можно исключить из GeoIP-фильтрации отдельные IP-адреса или подсети.

Next

Прошедший GeoIP-фильтрацию трафик обрабатывается другими подсистемами межсетевого экрана.

ViPNet xFirewall xF65000 Межсетевой экран для защиты ЦОДов

инфотекс

Исполнение xF65000

- 2U платформа производства «Аквариус»
- 4 x 1Gb RJ-45
- 4 x 1Gb SFP
- 8 x 10Gb SFP+
- 2 БП

Новые возможности

1

Высокая производительность
85 тыс. правил
DPI+IPS без деградации

2

HA-Cluster
Синхронизация сессий

Переключение за 1 сек

3

Динамическая маршрутизация
BGP
OSPF

4

Шлюзовой антивирус
Прокси-сервер
Поддержка ICAP

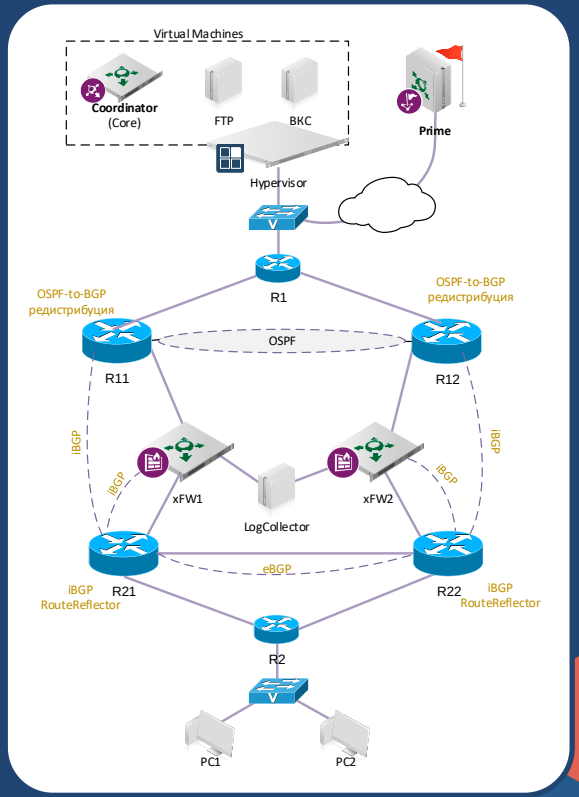
5

Резервирование
2 блока питания

Поддержка BFD

BGP. Моделирование переключения кластера

- Отключение питания активной ноды xFW1
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер BKC\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился
- Включение питания активной ноды xFW 2
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер BKC\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился



Сравнение производительности

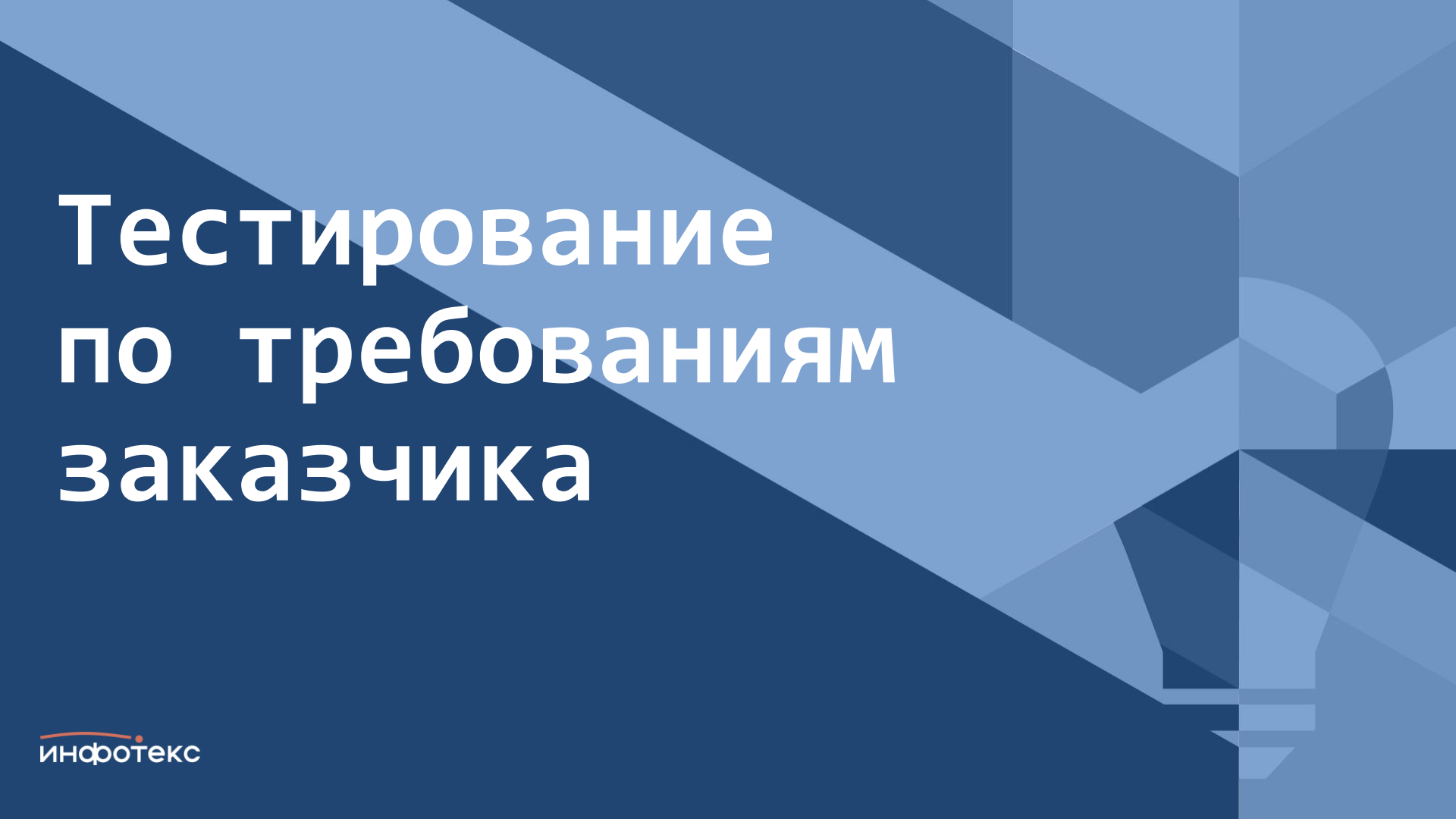
Checkpoint 28000

Firewall	Next Gen Firewall
145 Гбит/сек	51,5 Гбит/сек

ViPNet xFirewall xF65000

Firewall	Next Gen Firewall
76 Гбит/сек	60 Гбит/сек

Тестирование по требованиям заказчика



инфотекс

Условия тестирования

Протокол/Приложение	Порт	Доля Throughput, %
HTTPS	TCP/443	32,26
SMB/CIFS (MS DS)	TCP/445	30,48
HTTP	TCP/80	5,37
Citrix	TCP/1494	6,94
RDP	TCP/3389	1,4
DNS	UDP/53	0,3
SNMP	UDP/161	1
Syslog	UDP/514	6,89
MS SQL	TCP/1433	9,7
Имитация VNC	TCP/8080	5,66

Проведенные тесты

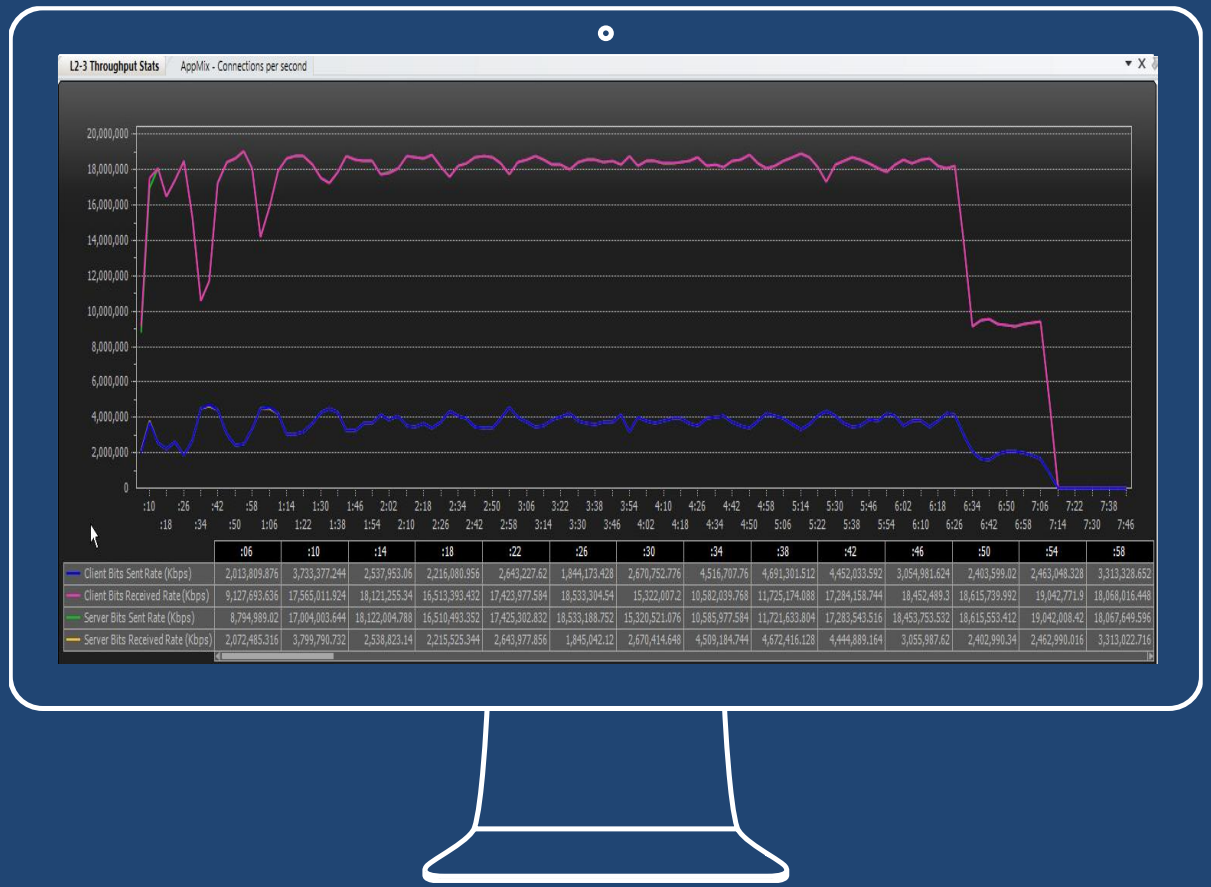
Номер теста	Характеристика набора правил				Ожидаемая пропускная способность, не менее, Гбит/с	Зафиксированы результаты, Гбит/с
	Количество правил, не менее	Срабатывающее правило	IPS	DPI		
1	85 000	все	нет	да	20	22
2	85 000	все	да	да	10	12
3	85 000	последнее	нет	да	20	22
4	85 000	последнее	да	да	10	12

	4:14	4:16	4:18	4:20	4:22	4:24	4:26	4:28	4:30	4:32	4:34	4:36	4:38	4:40	4:42
Client Bits Sent Rate (Kbps)	3,791,673.104	3,641,340.152	4,019,517.072	3,490,106.256	3,656,798.408	3,477,721.088	4,064,364.52	3,387,816.32	3,875,957.76	3,869,789.272	3,609,409.768	3,828,548.408	4,073,396.712	3,481,603.44	3,786,496.752
Client Bits Received Rate (Kbps)	18,464,135.784	18,571,269.776	18,455,706.68	18,502,321.256	18,439,365.56	18,706,366.016	18,308,229.584	18,689,884.664	18,528,874.392	18,217,725.168	18,489,626.488	18,470,325.528	18,166,094.92	18,508,100.136	16,986,823.264
Server Bits Sent Rate (Kbps)	18,463,868.128	18,572,071.112	18,457,765.984	18,502,062.56	18,438,326.32	18,706,757.224	18,308,085.4	18,690,700.768	18,527,843.688	18,223,780.424	18,490,462.984	18,471,700.192	18,167,438.56	18,508,673.712	16,995,707.312
Server Bits Received Rate (Kbps)	3,792,649.488	3,640,311.272	4,019,239.16	3,489,305.688	3,653,712.736	3,476,312.712	4,063,726.32	3,387,593.008	3,874,527.896	3,870,245.904	3,609,102.08	3,828,673.312	4,072,973.192	3,481,272.744	3,788,999.6

График теста №1

График теста №2

	5:34	5:38	5:42	5:46	5:50	5:54	5:58	6:02	6:06	6:10	6:14	6:18	6:22	6:26
Client Bits Sent Rate (Kbps)	2,402,467.44	2,684,556.652	2,720,825.78	2,629,699.276	2,568,169.636	2,904,204.392	2,688,693.692	2,686,762.296	2,486,396.964	2,760,101.076	2,611,524.396	2,718,202.768	2,425,156.348	2,616,753.728
Client Bits Received Rate (Kbps)	12,859,651.412	13,446,219.088	12,943,874.736	12,763,770.824	12,725,219.728	11,682,801.132	12,935,113.276	13,754,359.88	12,450,880.444	13,240,390.736	12,474,129.324	12,902,042.852	12,266,218.616	13,274,975.188
Server Bits Sent Rate (Kbps)	12,856,312.604	13,446,678.748	12,938,347.444	12,761,757.828	12,723,342.932	11,678,862.884	12,933,230.24	13,749,975.064	12,447,477.276	13,235,814.64	12,468,318.452	12,901,911.632	12,262,395.004	13,274,054.412
Server Bits Received Rate (Kbps)	2,402,920.356	2,684,896.524	2,716,137.724	2,628,462.84	2,563,625.68	2,903,890.872	2,690,059.252	2,687,642.444	2,485,279.136	2,755,799.704	2,610,362.924	2,720,082.148	2,422,233.652	2,615,842.696



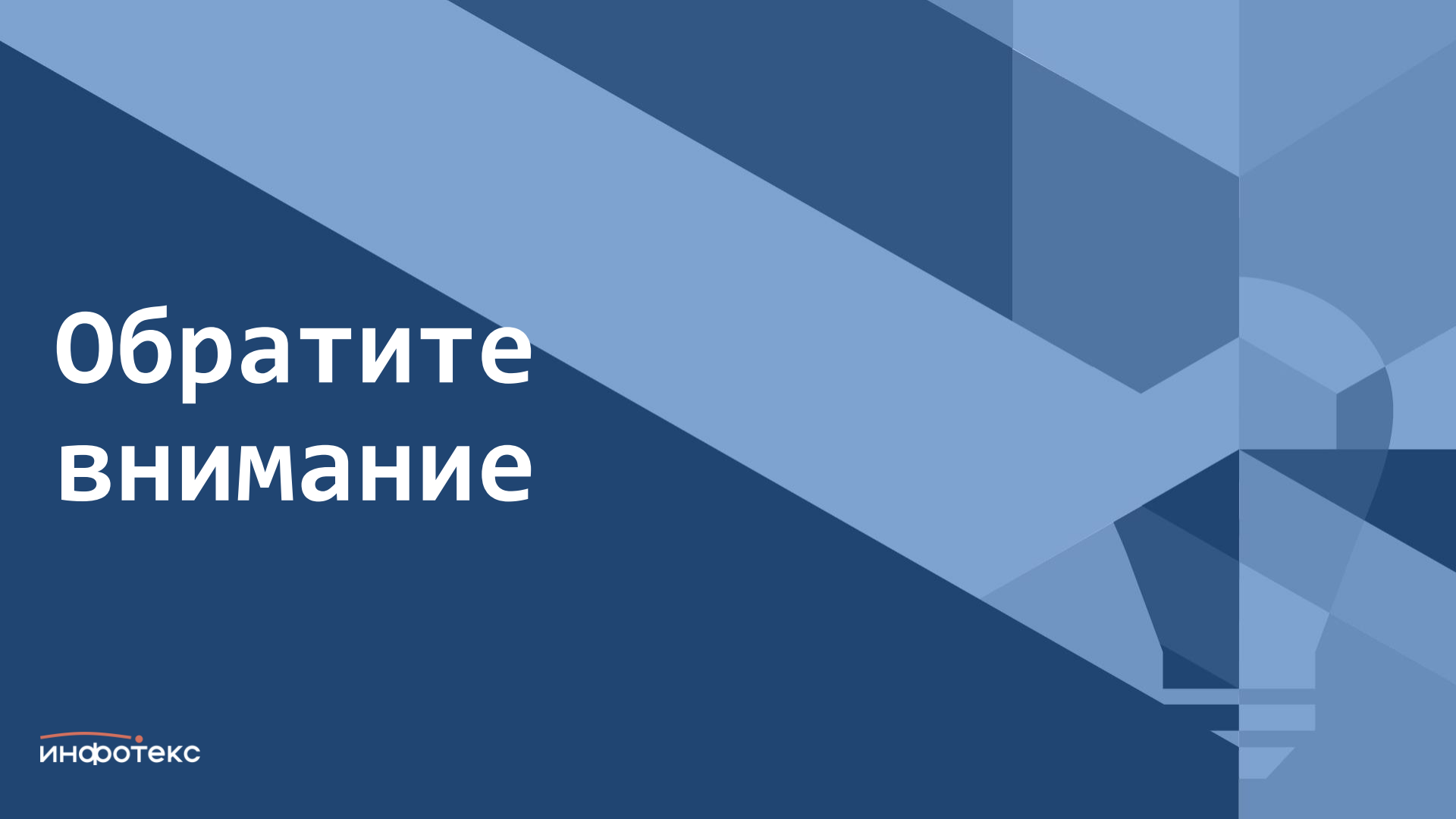
	:06	:10	:14	:18	:22	:26	:30	:34	:38	:42	:46	:50	:54	:58
Client Bits Sent Rate (Kbps)	2,013,809.876	3,733,377.244	2,537,953.06	2,216,080.956	2,643,227.62	1,844,173.428	2,670,752.776	4,516,707.76	4,691,301.512	4,452,033.592	3,054,981.624	2,403,599.02	2,463,048.328	3,313,328.652
Client Bits Received Rate (Kbps)	9,127,693.636	17,565,011.924	18,121,255.34	16,513,393.432	17,423,977.584	18,533,304.54	15,322,007.2	10,582,039.768	11,725,174.088	17,284,158.744	18,452,489.3	18,615,739.992	19,042,771.9	18,068,016.448
Server Bits Sent Rate (Kbps)	8,794,989.02	17,004,003.644	18,122,004.788	16,510,493.352	17,425,302.832	18,533,188.752	15,320,521.076	10,585,977.584	11,721,633.804	17,283,543.516	18,453,753.532	18,615,553.412	19,042,008.42	18,067,649.596
Server Bits Received Rate (Kbps)	2,072,485.316	3,799,790.732	2,538,823.14	2,215,525.344	2,643,977.856	1,845,042.12	2,670,414.648	4,509,184.744	4,672,416.128	4,444,889.164	3,055,987.62	2,402,990.34	2,462,990.016	3,313,022.716

График теста №3

	:10	:14	:18	:22	:26	:30	:34	:38	:42	:46	:50	:54	:58	1:02
Client Bits Sent Rate (Kbps)	507,116.408	461,821.108	513,871.924	774,745.616	953,436.172	925,991.432	1,221,324.896	1,286,399.62	1,525,297.936	1,734,121.816	2,313,988.364	2,456,650.152	2,268,742.704	2,496,589.896
Client Bits Received Rate (Kbps)	1,262,810.668	1,722,143.936	2,870,245.02	6,463,853.532	10,105,433.136	8,533,951.06	10,698,603.368	8,434,513.44	8,885,096.036	10,777,928.772	12,871,577.948	14,116,601.364	11,275,245.708	12,763,806.064
Server Bits Sent Rate (Kbps)	1,262,484.72	1,722,366.872	2,871,600.792	6,464,097.624	10,102,546.336	8,531,644.908	10,694,985.18	8,438,115.64	8,883,335.416	10,781,082.072	12,870,581.848	14,115,385.02	11,271,670.984	12,762,894.244
Server Bits Received Rate (Kbps)	505,588.596	462,701.588	514,451.084	774,597.068	953,723.172	926,033.424	1,226,075.08	1,288,399.584	1,525,975.24	1,734,699.808	2,313,596.208	2,456,894.54	2,268,054.02	2,497,102.292

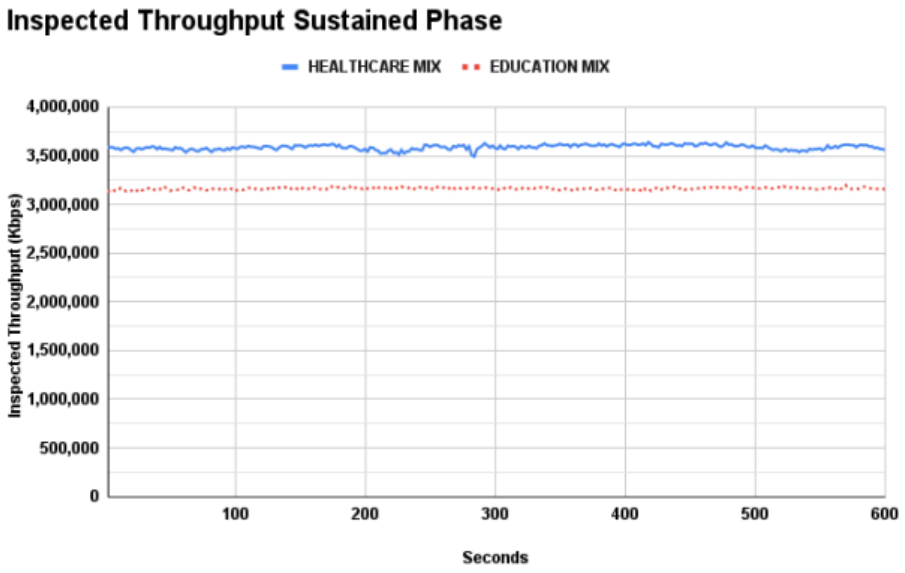
График теста №4

Обратите внимание



инфотекс

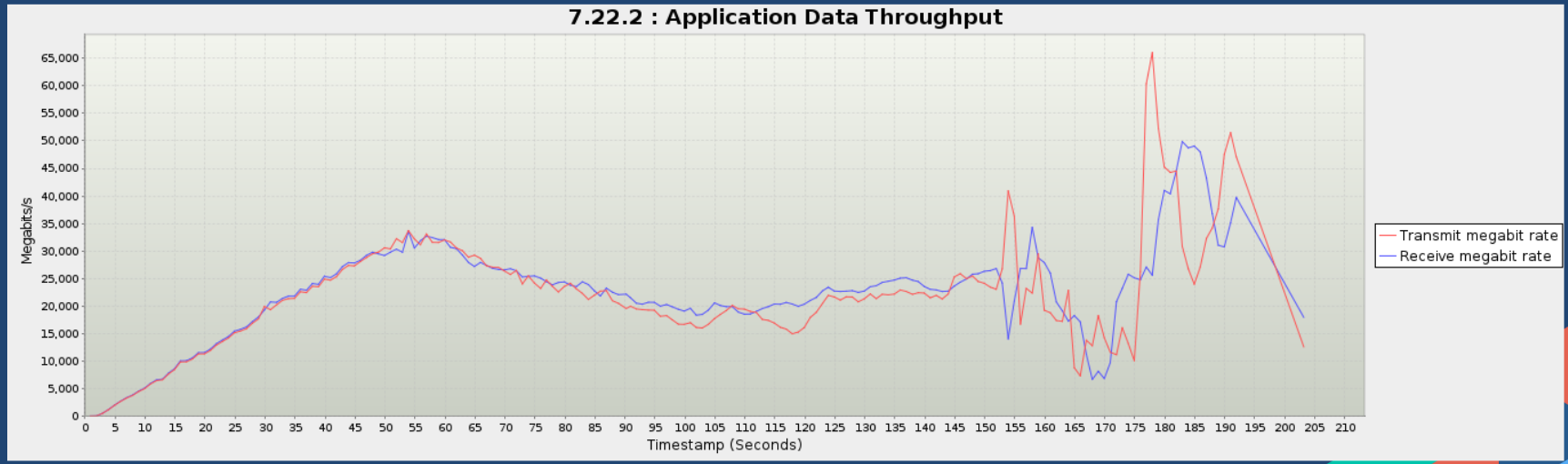
Это норма



Согласно RFC-9411, длительность теста должна быть не менее 300 секунд, без учета процесса «разгона» нагрузчика.

NetSecOPEN Certification Network Security Product Performance Testing Cisco Secure Firewall 3105

- Весь тест длился 205 секунд
- Из них 50 секунд стенд разгонялся
- Результаты колеблются от 7 до 70 Гбит/сек
- У теста нет стабильности



ViPNet xFirewall 6.0.0

инфотекс

Основные возможности 6 поколения

1

Standalone лицензия
Активация серийного номера через Интернет

2

Повышение производительности
В 6-10 раз зависит от теста

3

Динамическая маршрутизация
BGP
OSPF на базе FRR модуля

4

HA-Cluster
Синхронизация L7-сессий, переключение без перерыва сервисов

5

Новые NGFW функции
GeoIP, URL, Antivirus…

Первый релиз 6.0.0

Бета-версия – 19.12.2025

Обновление с xF 5 поколения на xF 6 поколения (локальное)

Обновление xF 6 поколения с версии 6.0.0 на последующие с помощью webUI

Новая ролевая модель

Экспорт/импорт индивидуальной конфигурации ПАК

Экспорт/импорт универсальной конфигурации ПАК

Сброс к заводским настройкам через GRUB

Общесистемные возможности

Первый релиз 6.0.0

Продолжение

Передача журналов (системных, пакетов) в множество систем, поддержка протокола tcp

Доработка отправки статистики по протоколу Netflow v9 во внешние системы

Возможность аутентификации по протоколу radius

Удаленное получение логов с резервной ноды

Ввод серийного номера ПАК в ходе эксплуатации для инвентаризации

Расширение параметров мониторинга здоровья

Общесистемные возможности

Первый релиз 6.0.0

Продолжение

Поддержка BGP, OSPF на базе FRR

Поддержка аутентификации в OSPF

Обнаружение недоступных шлюзов (DGD) на FRR

Политики маршрутизации (PBR) на FRR

Расширенная маршрутизация

Первый релиз 6.0.0

Продолжение

Повышение производительности для 85 тыс. правил для исполнений xF5000, xF65000

Реализация нового журнала ip-пакетов – журнала сессий

Выборочное журналирование для правил доступа

Запись IP-пакета в pcap по срабатыванию сигнатуры БРП

Использование профилей сигнатур IPS (mobile, Workstations, SCADA, VoIP и т.д.)

Потоковый Антивирус

Общесистемные возможности

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ИНФОТЕКС · TS Solution · AXOFT

Подписывайтесь на наши соцсети